TERRA VERDE

What Nobody is Talking About – The Potential Impact of the Equifax Breach on Small Business

by Tyler Rathjen | Oct 23, 2017 | Commentary, Terra Verde | 0 comments

What Nobody is Talking About – The Potential Impact of the Equifax Breach on Small Business

October is National Cyber Security Awareness Month and the Department of Homeland Security has been publishing various awareness content and resources out to the market for the last few weeks. We are taking a slightly different approach in our attempts to increase cyber awareness in the marketplace this month by publishing opinions and

CATEGORIES

Commentary
Compliance
Data Loss Management
Human Element of Security
IT Governance
Patching
Risk Management
Security Best Practices
Services
Solutions
Technology Partners
Terra Verde
Threat Updates
Uncategorized
Vulnerability Management

ARCHIVES

March 2018
February 2018
January 2018
December 2017

thoughts that are based on trends we have witnessed in the market over the last 12-18 months and some of the patterns we are beginning to see emerge around traditional criminal and cyber-attacks. The first series of blogs and research is around a topic that nobody appears to be talking about in relation to the Equifax breach which is: **The Equifax and EDGAR Breaches and Cryptocurrency Inflation.**

We hope you find this 3-part series engaging and thought provoking.

PART 1: THE EQUIFAX AND EDGAR BREACHES AND CRYPTOCURRENCY INFLATION

On September 7, 2017 Equifax reported that it was a victim of a data breach and communicated that 143 million American consumers and certain U.K., Canadian citizens were affected.

An enormous wave of online and printed articles, papers, and interviews discussing the breach swept over the globe following the announcement. A large majority of the articles and interviews discussed the potential impact that the breach would have on consumers, what consumers

November 2017
October 2017
September 2017
August 2017
July 2017
June 2017
May 2017
April 2017
March 2017
February 2017
January 2017
December 2016
November 2016
October 2016
September 2016
August 2016
July 2016
June 2016
May 2016
April 2016
March 2016
February 2016
September 2015
August 2015

can and should do to reduce the risk of theft, fraud and identity theft and how consumers can protect their identity and personal information going forward.

The media did a great job sensationalizing the breach – perhaps too good of a job, as Equifax's internal breach / customer support response process began to crumble due to the overwhelming number of emails, website visits and calls from angry and concerned consumers. No amount of disaster or breach recovery testing simulations could prepare Equifax for the onslaught of calls and emails that befell them.

On September 20th, nearly 2 weeks after the news of the Equifax breach was disclosed, SEC Chairman Jay Clayton released an eight-page statement that announced a 2016 breach of the EDGAR platform, that is used to store detailed financial reports on publicly traded companies.

It was reported that the EDGAR hack resulted from a "software vulnerability" in the system's test-filing component that "[was] exploited and resulted in access to nonpublic

information." Clayton also commented, "Notwithstanding our efforts to protect our systems and manage cybersecurity risk, in certain cases cyber threat actors have managed to access or misuse our systems."

The congressional watchdog Government Accountability Office also reported that the SEC wasn't always using encryption, supported software, well-tuned firewalls, and other key security tools while going about its business. According to Clayton, the company didn't discover until last month that the breach could have provided the information needed to make illegal trades.

It appears that both breaches were due to software vulnerabilities and a lack of basic IT protocol and best practices around patching and patch management.

WHAT HAPPENS NEXT?

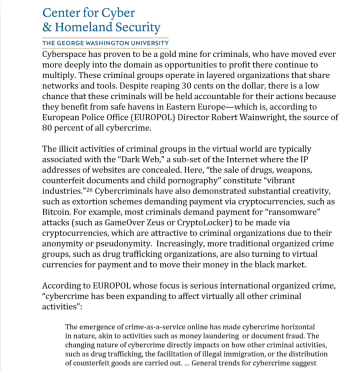
Equifax was quick to announce and promote a 90-day fraud alert program and their ability to enable consumers to implement a Security Freeze on their accounts. The fraud alert program forces a lender to take steps to gain

authorization from the credit holder prior to issuing a new line of credit or adjusting an existing line of credit. A security freeze prevents anyone but the consumer from viewing the credit report. It also means no one can access the credit report or make changes to it. For example, if you apply for a credit card or auto loan, a lender will need permission from the consumer before they can gain access to the credit report.

These recommendations do not prevent the consumer's personal information including social security and drivers license numbers, and employment and credit history from being published and sold on the dark web. The recommendations also do nothing to slow down cyber-criminals from stealing someone's identity and creating counterfeit legal documents, IDs or passports that could be used to open foreign bank accounts, fraudulently purchase goods and services, or establish online and physical businesses for criminal activities or money laundering purposes.

These are events that are occurring every day on the dark web – and have been

for some time. See this excerpt from "A Global Perspective on Cyber Threats" that was the testimony of Frank J. Cilluffo Director, Center for Cyber and Homeland Security to the U.S. House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations June 16, 2015.



Center for Cyber
& Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

Cyberspace has proven to be a gold mine for criminals, who have moved ever more deeply into the domain as opportunities to profit there continue to multiply. These criminal groups operate in layered organizations that share networks and tools. Despite reaping 30 cents on the dollar, there is a low chance that these criminals will be held accountable for their actions because they benefit from safe havens in Eastern Europe—which is, according to European Police Office (EUROPOL) Director Robert Wainwright, the source of 80 percent of all cybercrime.

The illicit activities of criminal groups in the virtual world are typically associated with the "Dark Web," a sub-set of the Internet where the IP addresses of websites are concealed. Here, "the sale of drugs, weapons, counterfeit documents and child pornography" constitute "vibrant industries."[24] Cybercriminals have also demonstrated substantial creativity, such as extortion schemes demanding payment via cryptocurrencies, such as Bitcoin. For example, most criminals demand payment for "ransomware" attacks (such as GameOver Zeus or CryptoLocker) to be made via cryptocurrencies, which are attractive to criminal organizations due to their anonymity or pseudonymity. Increasingly, more traditional organized crime groups, such as drug trafficking organizations, are also turning to virtual currencies for payment and to move their money in the black market.

According to EUROPOL whose focus is serious international organized crime, "cybercrime has been expanding to affect virtually all other criminal activities":

> The emergence of crime-as-a-service online has made cybercrime horizontal in nature, akin to activities such as money laundering or document fraud. The changing nature of cybercrime directly impacts on how other criminal activities, such as drug trafficking, the facilitation of illegal immigration, or the distribution of counterfeit goods are carried out. ... General trends for cybercrime suggest

Cyber-criminals, hacktivists, nation-states and organized crime syndicates have integrated their activities through the dark web. *Terra Verde has been publicly speaking about this level of integration and the new wave of crime-as-a-service offerings within the dark web for over 18 months*. We feel strongly that the Equifax attack and breach is only one of the key building blocks within a larger globally orchestrated attack that is potentially

designed to destabilize sections of the global economy and disrupt or change the balance of power (credit, currency, buying power, real estate).

We can speculate that the EDGAR breach was another key building block within the larger attack strategy as the breach could have been leveraged by cyber-criminals, hacktivists, nation-states or the criminal underground to make illegal trades using insider information, to validate how easy it is to facilitate illegal trades with non-public insider information, and generate wealth to fund cyber and physical criminal activities – globally.

During this same time, cryptocurrencies have been spiking in value even while the heads of global financial and investment corporations are denouncing cryptocurrencies and warning the public not to invest in these currencies. You could speculate that specific cryptocurrencies or that market in general is being manipulated by 3rd parties to cause the massive inflation of value on cryptocurrencies that are backed by no physical tangible assets.

These two breaches and the hyper-inflation of cryptocurrencies could be connected, and could be used to fulfill a strategic objective of undermining consumer and corporate confidence in certain government, banking and financial industry segments across the free world. These trends more than likely will have immediate, near term impact on businesses globally and will cause business owners and executives to rethink credit, payment and currency options and how they view and mitigate business and financial risk.

Please tune into our blog or follow Terra Verde on Linkedin to access latest news and Part 2 of this Series: *The Potential Impact of Equifax and EDGAR Breaches on Business.*

More

Home Page

Site Map
Internships
Contact
Privacy Policy

Our Company

Terra Verde□□
20601 N. 19th Avenue, #150
Phoenix, AZ 85027
Phone:+1 (877) 707-7997
Fax: 864-752-3491
Email: info@TVRMS.com
Map: Show me on Google Maps

Who We Are

Terra Verde provides sustainable Cybersecurity, Risk and Compliance Services and Solutions to organizations across the globe.

Connect with Us